Claims

[c1]   A smartcard transaction system configured with a biometric security system, said system comprising:

a smartcard configured to communicate with a reader;

a reader configured to communicate with said system;

a keystroke scan sensor configured to detect a proffered keystroke scan sample, said keystroke scan sensor configured to communicate with said system; and,

a device configured to verify said proffered keystroke scan sample to facilitate a transaction.

[c2]   The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3]   The smartcard transaction system of claim 1, wherein said keystroke scan sensor is configured to facilitate a finite number of scans.

[c4]   The smartcard transaction system of claim 1, wherein said keystroke scan sensor is configured to log at least one of a detected keystroke scan sample, processed keystroke scan sample and stored keystroke scan sam-

ple.

[c5] The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered keystroke scan samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The smartcard transaction system of claim 4, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c7] The smartcard transaction system of claim 5, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The smartcard transaction system of claim 1, wherein said keystroke scan sensor device is configured with at least one of an electronic sensor, an optical sensor and a keyboard.

[c9] The smartcard transaction system of claim 1, wherein said keystroke scan sensor is configured to detect and verify keystroke scan characteristics including at least one of behavioral, temporal and physical characteristics.

[c10] The smartcard transaction system of claim 1, wherein said keystroke scan sensor device is configured to detect false keystrokes and body heat.

[c11] The smartcard transaction system of claim 1, further including a device configured to compare a proffered keystroke scan sample with a stored keystroke scan sample.

[c12] The smartcard transaction system of claim 11, wherein said device configured to compare a keystroke scan sample is at least one of a third-party security vendor device and local CPU.

[c13] The smartcard transaction system of claim 11, wherein a stored keystroke scan sample comprises a registered keystroke scan sample.

[c14] The smartcard transaction system of claim 13, wherein said registered keystroke scan sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c15] The smartcard transaction system of claim 14, wherein

different registered keystroke scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c16] The smartcard transaction system of claim 14, wherein a keystroke scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a keystroke scan sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than

said first user information.

[c17]   The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered keystroke scan sample.

[c18]   The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered keystroke scan sample.

[c19]   The smartcard transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c20]   The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c21]   The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c22]   A method for facilitating biometric security in a smart-card transaction system comprising: proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification of a keystroke

scan sample for facilitating authorization of a transaction.

[c23] The method for of claim 22, further comprising registering at least one keystroke scan sample with an authorized sample receiver.

[c24] The method of claim 23, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a keystroke scan to said authorized sample receiver, processing said keystroke scan to obtain a keystroke scan sample, associating said keystroke scan sample with user information, verifying said keystroke scan sample, and storing said keystroke scan sample upon verification.

[c25] The method of claim 22, wherein said step of proffering includes proffering a keystroke scan to at least one of an electronic sensor, an optical sensor and a keyboard.

[c26] The method of claim 22, wherein said step of proffering further includes proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said keystroke scan sample.

[c27] The method of claim 22, wherein said step of proffering a keystroke scan to a keystroke scan sensor communi-

cating with said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c28] The method of claim 22, wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification further includes comparing a proffered keystroke scan sample with a stored keystroke scan sample.

[c29] The method of claim 28, wherein said step of comparing includes comparing a proffered keystroke scan sample to a stored keystroke scan sample by using at least one of a third-party security vendor device and local CPU.

[c30] The method of claim 28, wherein said step of comparing includes comparing keystroke scan characteristics including at least one of behavioral, temporal and physical characteristics

[c31] The method of claim 22, wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system further comprises using said keystroke scan sensor to detect at least one of false keystrokes and body heat.

[c32]   The method of claim 22, wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered keystroke scan sample.

[c33]   The method of claim 22, wherein said step of proffering a keystroke scan to a keystroke scan sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

[c34]   A method for facilitating biometric security in a smartcard transaction system comprising:
detecting a proffered keystroke scan at a sensor communicating with said system to obtain a proffered keystroke scan sample;
verifying the proffered keystroke scan sample; and
authorizing a transaction to proceed upon verification of the proffered keystroke scan sample.

[c35]   The method of claim 34, wherein said step of detecting further includes detecting a proffered keystroke scan at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

[c36]   The method of claim 34, wherein said step of detecting a

proffered keystroke scan includes detecting a proffered keystroke scan at least one of an electronic sensor, an optical sensor and a keyboard.

[c37]   The method of claim 34, wherein said step of detecting includes at least one of: detecting, storing, and process-ing a proffered keystroke scan sample.

[c38]   The method of claim 34, wherein said step of detecting further includes receiving a finite number of proffered keystroke scan samples during a transaction.

[c39]   The method of claim 34, wherein said step of detecting further includes logging each proffered keystroke scan sample.

[c40]   The method of claim 34, wherein said step of detecting further includes at least one of detecting, processing and storing at least one second proffered keystroke scan sample.

[c41]   The method of claim 34, wherein said step of detecting further includes using said keystroke scan sensor to de-tect at least one of false keystrokes and body heat.

[c42]   The method of claim 34, wherein said step of verifying includes comparing a proffered keystroke scan sample with a stored keystroke scan sample.

[c43]   The method of claim 42, wherein said step of comparing a proffered keystroke scan sample with a stored keystroke scan sample comprises storing, processing and comparing at least one of behavioral, temporal and physical characteristics.

[c44]   The method of claim 42, wherein comparing a proffered keystroke scan sample with a stored keystroke scan sample includes comparing a proffered keystroke scan sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

[c45]   The method of claim 34, wherein said step of verifying includes verifying a proffered keystroke scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c46]   The method of claim 34, wherein said step of verifying includes verifying a proffered keystroke scan sample using at least one of a local CPU and a third-party security vendor.